UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/884,672	06/19/2001	Tetsuya Noguchi	JP920000134US1	4503

7590 07/15/2005

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. Box 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/884,672	NOGUCHI ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-16,18-28,30-35 and 37-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-16,18-28,30-35 and 37-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 4/5/2005 have been entered and carefully considered.
2. The Amendment introduces a new limitation into claims 1, 4, 6-7, 9-13, 16, 18-19, 21-25, 28, 30 and 32. The newly introduced limitation has required a new search and consideration of the pending claims. The new search has resulted in newly discovered prior art. New grounds of rejection based on the newly discovered prior art follow below.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. *Applicant argues that Vainio does not teach that two send/receive devices generate verification data and send that data to their respective output devices, after which the data is compared.*
6. Applicant's argument has been carefully considered but it was not found persuasive. According to Fig. 6 wherein Vainio teaches Bluetooth authentication wherein a Device A sends RAND A to a Device B. This reads on sending data for verification data generation from one data send/receive device to the other send/receive device. Fig. 6 shows clearly shows that two devices generate verification data *(SRES)* and

each of them send that data out of the E1. Furthermore, the data is compared *(SRES ?=SRES).*

7. *Applicant argues that Vainio does not teach or suggest that a plurality of verification data values be generated and compared for mutual matches as is claimed.*
8. Applicant's argument has been carefully considered but it was not found persuasive. The examiner points out that *Vainio's* invention is clearly intended to devices of multiple use wherein the authentication scheme as disclosed in Fig. 6 is repeated numerous times resulting in generation of a plurality of verification data values. In addition, since both devices use the same data for verification values, the same input to their authentication functions E1 and apply the same algorithms *(Fig. 6),* each time that the verification data is compared SRES=SRES *(in Device A)* means nothing less than that the verification data at the verification data output section of both the data send/receive devices mutually match.
9. *Applicant argues that Vainio does not suggests the means or steps for defining a function as an operator, establishing a serial sequence of operators, and letting an input to the serial sequence of operators be the data for verification.*
10. This limitation including the newly added limitations is addressed below.
11. *Applicant argues that Vanio does not teach applying second generation algorithms, in addition to the first generation algorithms to accomplish the claimed verification.*
12. Applicant's argument has been carefully considered but it was not found persuasive. First of all, the claim limitation challenged by applicant is not present in claims 9-12, 21-24, 33 and 38-41. Secondly, Vanio teaches applying second generation

algorithms in addition to the first generation algorithms e.g. E0 *(Fig. 5)* and E1 *(Fig. 6)*. Thirdly, *Schneier's* "Applied Cryptogrpahy: protocols, algorithms and source code in C" presents plenty of different generation algorithms. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use multiple generation algorithms. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase systems' security.

13. *Applicant argues that Vainio makes no mention of any output sections.*

14. Applicant's argument has been carefully considered but it was not found persuasive. Vainio's authentication process clearly shows data input provided to an authentication function E1 which produces an output ACO and SRES.

15. *Applicant argues that successive iterations of Vainio interactions are not the same as the one that is claimed since the generation of a plurality of verification data is not known.*

16. The respectfully examiner disagrees. Vainio teaches Bluetooth as a technology that enables devices to connect to each other. This discussion on authentication scheme is a generic discussion on how the devices authenticate with other devices. The authentication scheme as disclosed in Fig. 6 is repeated numerous times and as a result plurality of verification data is generated.

17. *Applicant argues the examiner's Official Notice that the stating that obviousness rejections cannot be maintained since "Windows does not display verification data" bur rather that it generates a message in response to entry of an invalid password.*

18. Applicant's argument has been carefully considered but it was not found persuasive. The examiner points out that even though the "Windows" example did not provide applicant with a satisfying presentation of audio and visual data verification it was only an example to show that even in the most common situations (e.g. logging into one of the most used computer platforms) one is presented with visual and audio verification outputs for usability and security purposes. However, regardless of how satisfied applicant is with the example, it still does not change the fact that audio and visual verification data is old and well-known. As a result, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate audio, visual or audio and visual verification data for benefit of system's usability and security.

Although, applicant did not challenge the examiner's Official Notice examiner offers *Petrovich et al. (U.S. Patent No. 6101483, col. 9 lines 22-24)* and *Shrader et al. (U.S. Patent No. 6151599, col. 5 lines 43-46)* for more literal mapping of the claims' limitations.

19. Lastly, applicant's argument that *Davis* and *Narayanaswami* and *Lin* art would not be appropriate to arrive at the invention as claimed simply because none of these references teaches or suggests the means and steps for generating a plurality of verification data... etc. is not understood since the presented art even though not the same is analogues and complementary to *Vanio's.*

20. Claims 1-4, 6-16, 18-28, 30-35, 37-41 have been examined.

21. Claims 4, 6-7, 16, 18-19 and 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

22. Applicant canceled claims 5, 17, 29, 36 and 42-43. As a result, the suggestion that claims 1-43 "are currently pending" is inaccurate.

23. The meaning of phrases "defining a numeric on which the operator operates as an input to the operator" and "defining an operation result of the operator as an output of the operator" is not clear. The phrases are treated as best understood.

24. Claims 1, 13, 25, 30-31 and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Vainio (Juha T. Vainio, "Bluetooth Security").

25. As per claim 13 Vainio teaches Bluetooth authentication wherein a Device A sends RAND A to a Device B (Fig. 6). This reads on sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection.

26. Furthermore, Vainio teaches authentication function E1 in the Device A is used to create SRES' using RAND A (Fig. 6). This reads on generating verification data in the one data send/receive device, from the sent data for verification data generation produced using a first generation algorithm.

27. Similarly, the Device B derives SRES using RAND A and applying E1 (Fig. 6). This reads on generating verification data in the other data send/receive device from the

received data for verification data generation produced by the first generation algorithm.

28. Fig. 6 shows SRES being sent from the Device B to the Device, A which verifies whether SRES' and SRES match. This reads on determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.

29. Vainio does not explicitly teach outputting the generated verification data to its own verification data output section by each of the devices. However, this feature is inherent. E1 represents the authentication function and generated output ends up in a (verification data output) section of the device comprising the E1.

30. Vainio teaches Bluetooth as a technology enabling devices to connect to each other and his discussion on the authentication scheme is a generic discussion on how the devices authenticate with other devices. Vainio's invention is clearly intended to devices of multiple use wherein the authentication scheme as disclosed in Fig. 6 is repeated numerous times resulting in generation of a plurality of verification data values. In addition, since both devices use the same data for verification values, the same input to their authentication functions E1 and apply the same algorithms *(Fig. 6)*, each time that the verification data is compared SRES=SRES *(in Device A)* means nothing less than that the verification data at the verification data output section of both the data send/receive devices mutually match. This reads on "...the first generation algorithm generates a plurality of verification data, for each

verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually".

31. Claims 1, 25 and 30-31 are substantially equivalent to claim 13; therefore claims 1, 25 and 30-31 are similarly rejected.

32. Claims 2-3, 14-15 and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable *over Vainio (Juha T. Vainio, "Bluetooth Security")* in view of Official Notice.

33. Vainio teaches an ad-hoc radio communication as discussed above. Vainio does not explicitly teach that the verification data is visual and auditory verification data. Official Notice is taken that visual and auditory verification data is old and well-known. One of ordinary skill in art at the time of applicant's invention would use visual and auditory verification data to enhance a system's usability and security.

34. Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).*

35. As per claims 8 and 20 Vainio teaches data for verification data generation as discussed above. Vainio does not teach that the data for verification data generation is a public key of either data send/receive device.

Schneier teaches the data for verification data generation, which is a public key of either data send/receive device *(pg. 31 last §-pg. 32 §1-2).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a

public key of either data send/receive device as the data for verification data generation as taught by Schneier. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow communicated parties to solve a key-management problem *(Schneier, 32 § 2)*.

36. Claims 4, 6-7, 16, 18-19, 28 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Flanagan (David Flanagan, "Java in a Nutshell", 3rd Edition, 1999, ISBN: 1565924878)* and in further view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)*.

37. Vainio teaches a method and a system as discussed above.

38. Vainio does not teach defining a numeric, and defining an operation result of the operator.

39. *Flanagan* teaches defining an operation result of the *(e.g. pg. 142)* and a numeric *(e.g. the top of pg. 26 and Table 2-2 pg. 22)*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to define a numeric on which the operator operates as an input to the operator and an operation result of the operator as an output of the operator. One of ordinary skill in the art at the time of applicant's invention would have been motivated to perform such a modification in order to minimize the risk of instruction errors.

40. Vainio teaches algorithms E1 that operates on verification data RAND A and produces the verification data SRES as a result.

41. Vainio does not explicitly teach that the algorithm E1 is a one-way function.

42. *Schneier* teaches one-way functions *(pg. 29, One-Way Functions and pg. 351-353, Using One-Way Hash Functions).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the one way function in Vainio's invention as taught by *Schneier.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase the system's security.

43. One-way functions as taught by *Schneier* comprise a serial sequence of operators that are composed of two ore more of operators arranged in series, wherein the operators relate to the same or different one-way functions *(e.g. pg. 352)*, and wherein an output is created of two or more of operators selected from all operators composing the serial sequence of operators.

44. Claims 9-12, 21-24, 33-35 and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security") in view of Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)* and in further view of Davis et al. (U.S. Patent No. 6775770), *Narayanaswami (U.S. Pub. No. 20010013890) and Lin (U.S. Pub. 20020025046).*

45. Vainio teaches a method and system as discussed in reference to the previous claims.

46. As per claim 22 Vainio teaches a key exchange process wherein one of the devices sends information to another device and wherein the information is used to create a

symmetric encryption key *(Fig. 5)*. Vainio does not explicitly disclose that the authentication process precedes the key exchange process. However, Vanio teaches that authentication ensures the identity of a user. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to exchange keys after the users are authenticated. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid Man-in-the Middle Attack *(Schneier, pg. 48-49)*.

47. Vainio also does not teach each of the terminals transmitting the symmetric key Kc to the personal computer of each user, and thereafter both the personal computers sending and receiving data in cipher according to the symmetric key Kc. *Schneier* teaches two computers sending and receiving data in cipher using a symmetric key *(Schneier, pg. 28, § 1-2)* and teaches that exchanging the cipher key should be done using other communication channels than cipher data exchange (Schneier, pg. 176, last three §-pg. 177, first two §). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to employ Vanio's teaching to transmit the symmetric key to computers sending and receiving data in cipher according to the symmetric key Kc as taught by *Schneier*. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid eavesdropping *(Schneier, pg. 176, § 8)*.

48. Vainio does not teach the portable terminal of each user being connected to a personal computer of each user being connected by a secure communication path.

49. *Narayanaswami* teaches a terminal being connected to a personal computer by a secure path (high speed USB, *Narayanaswami [31].)*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to connect a portable terminal of each user to a personal computer of each user as taught by Narayanaswami. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow rapid transfer of data *[Narayanaswami, 31].*

50. *Davis et al.* teach a secure path *(Davis et al., Abstract).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to connect a portable terminal of each user to a personal computer of each user as taught by *Davis et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to provide the secure transfer of sensitive information *(Davis et al., Abstract).*

51. As per claim 21 Vainio does not teach a secret key being created by a personal computer of each user. Lin teaches that computing power, memory capacity and supply power of the portable device may not be sufficient for key generation *(Lin, [21]).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Vainio's invention so that the keys Kc are generated by the personal computers. One of ordinary skill in the art would have been motivated to perform such a modification in order to move key generation into the higher power and memory capacity devices.

52. Furthermore, Vanio in view of *Narayanaswami* do not teach using a received random number and an identifier for the second generation algorithm in producing the symmetric key Kc.

53. However, computer devices utilize various algorithms and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to send an identifier for the second generation algorithm in producing the symmetric key. One of ordinary skill in the art would have been motivated to perform such a modification in order to ensure the same results of algorithm calculations. Furthermore, Official Notice is taken that it is old and well-known practice to provide more than one numbers including a random number for symmetric keys generation. One of ordinary skill in the art at the time of applicant's invention would be motivated to deliver at least two numbers one of which would be a random number in order to increase key security while ensuring that the key derived on two different systems are the same.

54. Claims 9-12, 23-24, 33-35 and 38-41 are substantially equivalent to claims 21-22; therefore claims 9-12, 23-24, 33-35 and 38-41 are similarly rejected.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

7/8/05

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100